Department of Homeland Security Daily Open Source Infrastructure Report for 04 August 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The U.S. Food and Drug Administration announced Wednesday, August 2, that it has approved this year's seasonal influenza vaccines that include the new strains of virus judged likely to cause flu in the Northern Hemisphere in 2006−2007. (See item 24)
- USA Today reports an unusually hot summer has health officials concerned that the upcoming peak of the West Nile virus season could be worse than usual; the virus has already been detected in 33 states. (See item 25)
- The Baltimore Sun reports police are investigating a firebombing −− started by an incendiary device such as a Molotov cocktail −− at Baltimore Hebrew University on Wednesday, August 2, (See item 39)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *August 03, Associated Press* — **Swedish nuclear power plant alert.** Swedish nuclear authorities held an emergency meeting Thursday, August 3, after two reactors were shut down at a plant in the southeast of the country. The plant in Oskarshamn, about 250 kilometers (150 miles) south of the capital, Stockholm, shut down two of its three reactors late Wednesday after

the company running the plant reported that "safety there could not be guaranteed." The decision followed an incident last week at another nuclear plant in Sweden, in Forsmark, where backup generators malfunctioned during a power outage, forcing a shutdown of one of its reactors, said Anders Bredfell, a spokesperson for the Swedish nuclear authority, SKI. Bredfell said the reactors would remain shut until authorities determine whether the plant's backup generators could malfunction in the same way as at Forsmark. Greenpeace representative Martina Krueger said the incident in Forsmark, 75 kilometers (46 miles) north of Stockholm, was "serious" because it showed that a "meltdown" could easily happen. "When the generators could not kick in for emergency cooling, authorities realized there might be a problem in the battery system and that it might be generic to all reactors in the country," Krueger said.
Source: http://edition.cnn.com/2006/WORLD/europe/08/03/sweden.nuclea r.ap/

2. *August 03, Associated Press* — **Power demands remain high as heat wave fades.** Demand for electricity remained high as a heat wave began to fade under cooler air descending across upstate New York, but utilities reported no major outages Thursday, August 3. The Independent System Operator (ISO) forecast the third straight day of record power usage −− with 34,000 megawatts in the afternoon topping Wednesday's hourly average peak by 61 megawatts. The ISO initiated emergency steps for some major commercial and industrial customers in New York City and Long Island to shed more than 1,000 megawatts of demand. There were no major interruptions on the system since temperatures across most of the state rose into the 90s on Tuesday. National Grid, with nearly 1.6 million customers from Buffalo to Albany, reported lower demand Thursday after Wednesday's record. Most service was restored to the 20,000 customers in the Mohawk Valley who lost electricity in thunderstorms Wednesday afternoon, spokesperson Steve Brady said. Central Hudson Gas & Electric, with about 290,000 mid−Hudson Valley customers, also expected demand to drop below Wednesday's record. "The same as the previous days, there are minor scattered outages in our service territory but no major operational issues," spokesperson John Maserjian said.
Source: http://www.newsday.com/news/local/wire/newyork/ny−bc−ny−−hea twave−ny0803aug03,0,5484561.story?coll=ny−region−apnewyork

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

3. *August 03, Government Accountability Office* — **GAO−06−1006T: Department of Defense: Sustained Leadership is Critical to Effective Financial and Business Management Transformation (Testimony).** The Department of Defense (DoD) bears sole responsibility for eight DoD−specific high−risk areas and shares responsibility for six governmentwide high−risk areas. These high−risk areas reflect the pervasive weaknesses that cut across all of DoD’s major business operations. Several of the high−risk areas are inter−related, including, but not limited to, financial management, business systems modernization, and DoD’s overall approach to

business transformation. Billions of dollars provided to DoD are wasted each year because of ineffective performance and inadequate accountability. DoD has taken some positive steps to successfully transform its business operations and address these high−risk areas, but huge challenges remain. This testimony discusses (1) pervasive, long−standing financial and business management weaknesses that affect DoD's efficiency; (2) some examples that highlight a need for improved business systems development and implementation oversight; (3) DoD's key initiatives to improve financial management, related business processes, and systems; and (4) actions needed to enhance the success of DoD's financial and business transformation efforts.
Highlights: http://www.gao.gov/highlights/d061006thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−1006T

4. *July 26, Aviation Week* — **Military MRO forecast.** Military aircraft retirements will start outpacing deliveries in about three years and probably will continue doing so for the next decade, predicted Kevin Michaels, an AeroStrategy principal, at Aviation Week's Maintenance, Repair and Operations (MRO) Military Europe Conference. The global military aircraft fleet of Western aircraft numbers about 38,610, 92 percent of which are either "mature" (51 percent) or "old" (41 percent), according to the firm. The fleet will start getting younger as the oldest aircraft retire, with retirements peaking between 2010 and 2011, when more than 1,200 aircraft are scheduled to retire each year, according to Hal Chrisman, another AeroStrategy principal. Deliveries will climb a bit between 2009 and 2011 because of increased deliveries from aircraft such as the Bell 407, UH−60, F−35, A400M, NH−90 and V−22. However, by 2013 deliveries dip below 1,000 annually and then slowly slide to around 800 by 2016. Although the size of the fleet is expected to decline 1 percent per year over the forecast period, support costs are increasing 2 percent because of greater system complexity, said Chrisman. For instance, mission−critical equipment in fighters usually are loaded with electronics that typical transport aircraft don't have, so it tends to be more expensive.
Source: http://www.aviationnow.com/avnow/news/channel_om_story.jsp?id=news/om706milf.xml

[Return to top]

Banking and Finance Sector

5. *August 03, Sydney Morning Herald (Australia)* — **Identity theft virus infects 10,000 computers.** More than 10,000 Australian computers have been infected by a Trojan virus −− invisible to most anti−virus software −− that is transmitting their owners' private details to identity thieves. The Australian Tax Office confirmed Wednesday, August 2, that 178 taxpayers had unwittingly revealed their tax file numbers while lodging tax returns online. The Tax Office was warned of the infection by the Australian Computer Emergency Response Team (Auscert), which has been issuing similar warnings to banks and other large organizations whose clients' details have been compromised. A security analyst at Auscert, MacLeonard Starkey, said the "Haxdoor" Trojan could log keystrokes from computers, capture usernames and passwords stored in the Windows operating system and harvest data being transmitted from a computer during the completion of online forms such as tax returns. Starkey said tax file numbers, bank account details, and other personal data could be used by criminals to steal identities, to raid bank accounts or to lodge false tax returns. He said that commonly used anti−virus programs

could not detect the Trojan, which had been invented by a Russian programmer who sold it commercially under the name "A311 Death".
Source: http://www.smh.com.au/articles/2006/08/02/1154198204613.html

6. *August 02, United Press International* — **Counterfeit money hits France.** European countries, especially France, reportedly are being hit by fake money as counterfeiters seem to have found the code for the euro. Britain's Independent newspaper reports in the first six months of this year, 300,000 fake euro notes −− 30 percent of them in France −− were taken out of circulation. Most of the notes were printed in other countries. The euro, supposedly the most difficult currency to counterfeit, was introduced in 12 countries in January 2002. The Independent report said counterfeiters in Europe and outside may have cracked the currency's code.
Source: http://www.upi.com/NewsTrack/view.php?StoryID=20060802−11013 0−5507r

7. *August 02, Poughkeepsie Journal (NY)* — **Stolen hospital laptop had patient data dating back to 2000.** A computer containing personal identification information of 257,800 Vassar Brothers Medical Center patients was stolen in June, hospital officials said. The laptop computer was taken from the emergency department sometime between June 23 and June 26. It contained information on hospital patients dating back to 2000, but only had personally identifying information such as Social Security numbers and dates of birth for 257,800, officials said. The center notified those patients with a letter dated July 17. The letter stated that the computer was password protected and there is "no evidence that the hard drive has been inappropriately accessed." The laptop computer is used to gather initial patient information at people's bedsides. It was secured by a cable lock to a mobile cart in the emergency department.
Source: http://www.poughkeepsiejournal.com/apps/pbcs.dll/article?AID=/20060802/BUSINESS/60802004

8. *August 02, Clarion Ledger (AL)* — **Belhaven College data stolen.** A laptop computer stolen last month from a Belhaven College employee contained names and Social Security numbers of college employees, leaving them vulnerable to identity theft. Belhaven College President Roger Parrott confirmed Tuesday, August 1, the stolen computer contained some personal information on employees. But Parrott said he didn't know how many of the private school's roughly 300 employees' personal information was compromised by the theft. Parrott notified faculty and staff of the situation in a memo July 25. "The computer of the auditor did have several sophisticated levels of security on it," Parrott said. The robbery at Belhaven, which is located in Alabama, happened on July 19, when a school employee was walking to his car after work. A man approached him from behind. The man took the employee's wallet and laptop computer then fled. As of late Tuesday, no arrest had been made.
Source: http://www.clarionledger.com/apps/pbcs.dll/article?AID=/20060802/NEWS/608020375

9. *August 02, The Herald (South Africa)* — **Rise in explosives attacks on South African ATMs causes concern.** Absa, a South African bank offering large commercial, private, and Internet banking, on Tuesday, August 1, raised concerns over the increase in incidents in which explosives are used to blow open ATMs. Criminals had blown up a “handful” of Absa ATMs in the last month. In the most recent incident, thieves used commercial explosives to blow up an ATM to steal an undisclosed amount of cash in Kwa−Thema, on the East Rand, South Africa, on Sunday, July 30. Two weeks prior, another ATM was blown up.

Source: http://www.theherald.co.za/herald/news/n05_02082006.htm

10. *August 02, VNUNet* — **Huge botnet swamps UK firms with eight million phishing e−mails.** Security experts Wednesday, August 2, warned that a single botnet is being used to bombard UK firms with millions of phishing e−mails. According to BlackSpider Technologies, the huge botnet of zombie computers controls more than 20,000 distinct IP addresses. It began sending out the phishing emails on Sunday, and over 24 hours the security firm estimates it sent out more than 8.1 million e−mails. The subject lines of the emails invariably refer to either NatWest or Bank of Scotland. The phishing e−mails contain an inline image and if recipients click on the image, they are directed to a Website where they are instructed to input their personal information. Once entered, the information can then be used by the cyber criminals behind the attack to siphon cash from victims' bank accounts. James Kay, CTO, BlackSpider Technologies, said: "In security terms, phishing attacks are nothing new. What we're not used to seeing, however, is such a high volume of phishing e−mails being directed by one source."
Source: http://www.vnunet.com/vnunet/news/2161530/huge−botnet−swamps −uk−firms

11. *August 02, IDG News Service* — **FBI joins with industry to tackle ID theft.** The U.S. Federal Bureau of Investigation (FBI) is stepping up its fight against online fraud with a new initiative called Operation Identity Shield, according to a senior FBI official. The project, which is already in operation, is one of a growing number of collaborations between the FBI and the technology industry. "It's sort of an evolution of what we've seen in the phishing area," said Daniel Larkin, chief of the FBI's Internet Complaint Center, speaking at the Black Hat USA conference in Las Vegas on Wednesday, August 2. The FBI's antiphishing effort, called Digital PhishNet, was launched in late 2004 with backing from companies like Microsoft, America Online, and VeriSign, as well as the U.S. Secret Service and the U.S. Postal Inspection Service. The FBI plans to publicize Operation Identity Shield in the coming months, but already Larkin credits the effort as contributing to a number of arrests.
Source: http://www.pcworld.com/article/id,126632;c,cybercrime/articl e.html

[Return to top]

Transportation and Border Security Sector

12. *August 03, Associated Press* — **Wilson Bridge reopened after investigation.** Police have reopened Interstate 95 at the Woodrow Wilson Bridge on Thursday morning, August 3, after a suspicious device was pulled from the water under the bridge. Maryland State Police spokesperson Sergeant Thornnie Rouse says the device turned out to be a weather monitoring system. It was pulled from the water by construction crews at the bridge project. Rouse says the workers were alarmed because the device appeared to have batteries and wires attached to it. Rouse says the highway was closed on both sides of the bridge for about an hour and was reopened at 8:15 a.m. EDT.
Source: http://www.wusatv9.com/news/news_article.aspx?storyid=51186

13. *August 03, Cincinnati Enquirer* — **Comair faces new problems.** Comair's effort to emerge from bankruptcy faces a new setback, because two unions that ratified concessions back in January said Wednesday, August 2, that the deals are off. The regional airline's inability to cut a

deal with its flight attendants union for enough concessions violates a key promise in deals with the pilots and mechanics, the unions said. After a protracted court battle, Comair was authorized last month by a bankruptcy judge to throw out its flight attendant contract −− but it can impose only $7.9 million worth of concessions. That falls short of the $8.9 million in cuts from the flight attendants that were specified in both the pilot and mechanic deals, which were contingent on the flight attendant deal. The attendants union, however, has threatened work disruptions −− including a possible strike −− if Comair imposes new terms. Comair, a Delta Air Lines subsidiary, says it needs to cut its salaries and benefits to become competitive again and successfully bid for aircraft and routes that will jump−start growth.
Source: http://news.enquirer.com/apps/pbcs.dll/article?AID=/20060803/BIZ01/608030327/1076

14. *August 03, Atlanta Journal−Constitution* — **Atlanta airport unveils quicker baggage scanning system.** For the first time since stringent security measures were imposed at domestic airports after the 9/11 attacks, travelers using Atlanta's Hartsfield−Jackson International Airport will be able to check luggage at ticket counters, instead of lugging it to screening areas. "Now, just put it on the belt and it's gone," airport manager Ben DeCosta said Thursday, August 3, as airport officials showed off the new baggage screening system. The $170−million system began operating July 6 in the North Terminal, which serves a variety of airlines, including AirTran, and should be completely operational in six weeks at the South Terminal, which is used mostly by Delta Air Lines, said airport spokesperson Felicia Browder. In June, the airport handled 1.2 million checked bags and averages about one million per month, DeCosta said. The screening system can handle more than 1,800 bags per hour. It has five miles of conveyor belts and a new lineup of X−ray and CT scan machines to sort questionable bags. A Transportation Security Administration screener reads the image on a computer screen and flags anything that looks suspicious because of its shape, density or some other characteristic.
Source: http://www.ajc.com/metro/content/metro/atlanta/stories/0803a irport.html

15. *August 03, Associated Press* — **Amtrak cuts Acela speeds because of hot weather.** Because of the high heat conditions, Amtrak temporarily has cut speeds on its Acela trains from 135 miles per hour down to 80 miles per hour. Amtrak says the combination of high temperatures and high train speed could potentially damage the track. Amtrak says speed reductions can prevent damage, allow for better monitoring of changes in rail conditions, and prevent potential accidents.
Source: http://www.wavy.com/Global/story.asp?S=5234450&nav=23ii

16. *August 03, News Times (CT)* — **Danbury airport increases its security.** With upgraded fences and fewer access gates, the Danbury (CT) Municipal Airport has more security features now than when a man jumped over the airport fence and stole a plane more than a year ago. But other security upgrades recommended by a security specialist in January remain on the city's to−do list. Security at the airport received national attention in June 2005, when Philippe Patricio stole a single−engine plane and flew it to Westchester Airport in New York with two friends. Although the city airport met Federal Aviation Administration regulations for small airfields, city officials took initial steps to address security issues immediately following the incident, including the adjustment of schedules of special officers who patrol the airport. The city also hired an airport security specialist to figure out what more needed to be done. According the specialist's report, the city's airport needed better fences, new access gates, and a

high−tech swipe card system to control access, among other measures. Airport administrator Paul Estefan said Wednesday, August 2, that he had replaced worn fencing and removed four pedestrian gates to limit access to the airport.
Source: http://www.newstimeslive.com/news/story.php?id=1008728

[Return to top]

Postal and Shipping Sector

17. *August 03, Agence France−Presse* — **British police investigating explosives mailed to Labor Party.** Police are investigating an incident in which a "home−made" explosive device was sent to an office of the governing Labor Party in Cambridge, southeast England. The device, described by a police spokesperson as "an envelope within an envelope that had a cardboard tube inside which was about six inches long" packed with explosives. The "crude" device, currently being examined by explosives experts, arrived at the Cambridge Labor Party's office on Wednesday, August 2, and was discovered by a staff member who alerted the police. Chief Superintendent Rob Needle of the Cambridgeshire police constabulary said a number of other organizations and individuals in the area had also been sent "hate mail" in recent weeks, and said the police were investigating whether the incidents were linked.
Source: http://news.yahoo.com/s/afp/20060803/wl_uk_afp/britainpolicelabourexplosive_060803121837

[Return to top]

Agriculture Sector

18. *August 03, Summit Daily News (CO)* — **Scientists believe a disease is killing aspen trees.** While mountain pine beetles continue to ravage large swaths of forests in the West, the region's aspen groves are falling prey to an unknown disease that could wipe out 10 percent or more of the iconic trees. Dale Bartos, an ecologist with the U.S. Forest Service's Rocky Mountain Research Station in Logan, UT, said it's not clear what's causing the problem with the aspens, although unlike the beetles killing the pines, the aspens are likely being attacked by some kind of disease. Unlike many trees and plants, aspens don't reproduce sexually but, rather, through cloning from new shoots emerging from within their interconnected root systems. Bartos said researchers are seeing the trees' clones dying off completely so that stands can't regenerate themselves.
Source: http://www.summitdaily.com/article/20060802/NEWS/60802002/0/ FRONTPAGE

19. *August 02, Agence France−Presse* — **New case of mad cow disease confirmed in Azores.** A new case of mad cow disease has been confirmed in Portugal's Azores islands, the sixth known incidence of the disease there since November 2000, the regional government said. The presence of Bovine Spongiform Encephalopathy (BSE) −− known as mad cow disease −− was detected in screening tests and confirmed by the national veterinary laboratory. The cow on the island of Pico, part of the nine−island archipelago in the Atlantic Ocean, was a 15−year−old Holstein−Frisian, whose carcass was immediately destroyed in accordance with safety procedures. The Azores government also said it had ordered the slaughter of other animals in

contact with the infected cow.
Source: http://news.yahoo.com/s/afp/20060802/hl_afp/healthmadcowportugal_060802203016;_ylt=AumL2chB.v9UMQsc.RYGwgyJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

20. *July 28, Associated Press* — **Disease hits Michigan's cucumber crop.** A disease that attacks cucumbers has emerged for a second consecutive growing season in parts of the state, handing another hardship to Michigan's agricultural industry. Downy mildew has been confirmed in Allegan, Monroe and some other Michigan counties, as well as Ohio, Indiana and Ontario, Canada. But researchers say its presence could be more widespread. Michigan produces nearly one−third of the nation's crop of pickling cucumbers. "If you get it, it's a disaster," said Michael Hescott, president of Freestone Pickle Co. Without adequate prevention, "in six or seven days a field will be laid over dead. It looks like it's been hit by a hard frost."
Downy mildew information: http://web.aces.uiuc.edu/vista/pdf_pubs/927.pdf
Source: http://www.freep.com/apps/pbcs.dll/article?AID=/20060728/NEWS12/607280451/0/BUSINESS07

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

21. *July 28, Associated Press* — **Massachusetts sets state standard for perchlorate.** Massachusetts has become the first state to set a standard for the amount of a potentially dangerous chemical found in drinking water that is present in at least 25 states across the country. The new regulations announced Friday will require most public water systems to be tested regularly for the chemical perchlorate, which is produced naturally, but is also the byproduct of manufacturing and military operations. The chemical is of concern because it interferes with pre− and postnatal thyroid functions, and can impair development and metabolism. The new regulation sets the perchlorate drinking water standard at two parts per billion, which is significantly lower than the U.S. Environmental Protection Agency's recommended reference dose of about 24 parts per billion.
Source: http://www.boston.com/news/local/massachusetts/articles/2006/07/28/massachusetts_sets_state_standard_for_perchlorate/

22. *July 19, Pittsburgh Tribune−Review* — **Pathogen lab will close.** The Special Pathogens Laboratory at the VA Pittsburgh Healthcare System, known worldwide for its groundbreaking research in Legionnaires' disease, will close Friday, July 19. Hospitals across the nation might be hard−pressed to find a laboratory to test for the deadly bacteria found in tap water. The lab's closing comes 30 years to the day after the event that gave Legionnaires' disease its name. A form of bacterial pneumonia, Legionnaires' is best known for a deadly outbreak that killed 34 people and sickened 221 others attending the 58th Pennsylvania American Legion Convention

in Philadelphia July 21−24, 1976. The VA research team is credited with later discovering that water is the source of the disease, developing testing and disinfection methods to prevent it, and finding the right antibiotics to cure it.
Source: http://www.pittsburghlive.com/x/pittsburghtrib/news/cityregi on/s_462453.html

[Return to top]

Public Health Sector

23. *August 04, Associated Press* — **Thai scientists say they have produced generic Tamiflu.** Thai scientists have successfully synthesized a generic version of the anti−viral drug used to treat bird flu in humans, and it will be distributed to health centers by November,officials said Thursday, August 3. The generic version of oseltamivir −− better known by the trademarked name Tamiflu −− is undergoing further tests at Bangkok's Siriraj Hospital. The capsule produced in Thailand will be called GPO−A−Flu, officials told a news conference in the capital. The Government Pharmaceutical Organization (GPO) expects to produce and distribute the medicine through the national public health system by November. The GPO will stockpile two million GPO−A−Flu capsules, but in the event of a large bird flu outbreak among humans, can produce up to 400,000 capsules per day, officials said.
Source: http://www.thejakartapost.com/detaillgen.asp?fileid=20060803 190409&irec=1

24. *August 02, U.S. Food and Drug Administration* — **Influenza vaccines to be manufactured for upcoming flu season approved.** The U.S. Food and Drug Administration (FDA) announced Wednesday, August 2, that it has approved this year's seasonal influenza (flu) vaccines that include the new strains of virus judged likely to cause flu in the Northern Hemisphere in 2006−2007. Each year influenza vaccine manufacturers submit information and samples to FDA of their virus strains being manufactured for the upcoming seasonal influenza season for review and testing in FDA laboratories. Because different influenza virus strains may appear each year, one or more of the strains in the vaccine may need to be changed to protect against what public health experts think are the strains most likely to infect people that year. This season's approved formulation for the U.S. vaccine is identical to that recommended by both the World Health Organization and FDA's Advisory Committee. The formulation includes one strain that was used in last year's vaccine and two new strains. Seasonal flu vaccines do not protect against avian flu, which is caused by different viral strains.
Source: http://www.fda.gov/bbs/topics/NEWS/2006/NEW01423.html

25. *August 01, USA Today* — **West Nile thriving in searing summer heat.** An unusually hot summer has health officials concerned that the upcoming peak of the West Nile virus season could be worse than usual. The virus has been detected in 33 states, which means "any area of the country is at risk," says Lyle Petersen, director of vector−borne infectious diseases at the U.S. Centers for Disease Control and Prevention (CDC). Last year, only 16 states had reported West Nile activity by the end of July, he said. "Right now, the number of cases is literally doubling or more every week," Petersen said. "What that's telling us is we're going to have another significant outbreak in this country this year."
West Nile virus information: http://www.cdc.gov/ncidod/dvbid/westnile/index.htm
Source: http://www.usatoday.com/news/health/2006−08−01−nile_x.htm

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

26. *August 03, Providence Journal (RI)* — **Special guard squad's debut showcases commando−style protection.** A team of specially−trained commandos −− whose mission is to assist first responders in an event of terrorist attack −− made its official debut Wednesday, August 2 outside the Rhode Island state National Guard headquarters. The 13th Weapons of Mass Destruction Civil Support, a full−time National Guard unit based in Coventry, RI, is ready for rapid deployment to support local, state and federal authorities in responding to any attack involving weapons of mass destruction. The 22−member squad, which earned national certification last week following a near three−year training period, is officially under the governor's command.
Source: http://www.projo.com/ri/coventry/content/projo_20060803_cv3t eam.1ee9eeb.html

27. *August 03, Federal Emergency Management Agency* — **Tropical Storm Chris updates −− Chris weakens.** At 5:00 am EDT, the center of Tropical Storm Chris was located near latitude 20.3 north longitude 66.4 west or about 315 miles east−southeast of Grand Turk Island and about 135 miles north of San Juan, Puerto Rico. Chris is moving toward the west near 13 mph. and this motion is expected to continue during the next 24 hours. On this track the center of Chris will be moving away from Puerto Rico and the Virgin Islands today. Maximum sustained winds have decreased to near 45 mph with higher gusts. Little change in strength is forecast during the next 24 hours. Tropical storm force winds extend outward up to 80 miles from the center. Chris is expected to produce total rainfall accumulations of three to five inches with isolated totals of 10 inches over the higher elevations of Puerto Rico. Total rainfall of two to four inches is possible over the Virgin Islands with possible isolated maximum amounts of six inches through today.
Source: http://www.fema.gov/emergency/reports/2006/nat080306.shtm

28. *August 02, Independent (NJ)* — **New Jersey county holds seminar on hurricane preparedness.** The midpoint of the hurricane season is just weeks away, and area officials are working to heighten awareness of preparation tactics for Monmouth County, NJ residents. A hurricane preparedness seminar took place July 24 at the American Red Cross headquarters with a panel discussion featuring emergency responders and weather experts on the local, state and national levels. The event, titled "Together We Prepare," was sponsored by the Rumson Borough Council and was moderated by Rumson Councilman Mark Rubin. Harry Conover, coordinator of emergency management for Monmouth County, said that the reality of a storm causing serious damage to all of New Jersey is something that government officials cannot ignore. Conover said that his main concern for how to prepare for a storm lies in how to evacuate or shelter special−needs cases. "We're looking to put together a roster of people with

special needs," he said, adding that the language barrier that exists between government officials and immigrants in the area, many of whom are undocumented, could count as a special need. Conover said that keeping the public informed is a top priority, given the fact that there are 650,000 people in Monmouth County and more than 350 schools.
Source: http://independent.gmnews.com/news/2006/0802/Front_Page/013. html

29. *August 02, Amarillo Globe News (TX)* — **Texas Panhandle drill to test response readiness.** On August 8 and 9, first responders across the Texas Panhandle will participate in an exercise to measure the area's readiness for mass disasters. Plans call for emergency scenarios to be played out but without sending teams into the field. "This is what is called a functional exercise," said Walt Kelley, emergency management coordinator for Amarillo and Potter and Randall counties. "Instead of seeing firemen running around, people will be handed a piece of paper with a situation on it and start from there." The idea is to practice responses without spending the large amount of money it would take to fully recreate an emergency.
Source: http://www.amarillo.com/stories/080206/new_5250843.shtml

30. *August 02, Illinois Government News Network* — **Illinois governor announces a major emergency response exercise.** Illinois Governor Rod R. Blagojevich announced on Wednesday, August 2, a major emergency response exercise beginning Friday, August 4 in the Metro East area will test the state's ability to respond to large−scale emergencies and for the first time will include a mass evacuation and sheltering component. The exercise will be the state's second significant emergency response exercise within the past three months. In May, the state conducted a three−day exercise that tested Illinois' ability to respond to simultaneous major emergencies, which included a pandemic flu outbreak and a terrorist attack centered in the Chicago metropolitan area. The exercise is designed to bring federal, state and local response organizations together in a coordinated response to multiple emergency scenarios. Exercise events on Friday will trigger a simulated evacuation and sheltering situation in Edwardsville, with mock evacuees being picked up and transported to the shelter at Liberty Middle School in Edwardsville. Other exercise scenarios during the five−day exercise include intelligence gathering and response to simulated terrorist attacks, distribution of materials from the Strategic National Stockpile (SNS), victim search and rescue efforts and establishment of a field hospital for treating "victims."
Source: http://www.illinois.gov/PressReleases/ShowPressRelease.cfm?SubjectID=1&RecNum=5133

[Return to top]

Information Technology and Telecommunications Sector

31. *August 03, VNUNet* — **Home users getting wise to Wi−Fi security.** Home users are becoming increasingly aware of Wi−Fi security, a new study has found. Sixty percent of wireless network owners implement security on their equipment, according to research firm Jupiter Research. Home users are most worried about privacy issues from leaving their network open and they're also concerned about illicit use and bandwidth theft.
Report is available for purchase at:
http://www.jupiterresearch.com/bin/item.pl/research:concept/ 625/id=97415/
Source: http://www.vnunet.com/vnunet/news/2161582/home−users−getting −wise−wi

32. *August 02, U.S. Computer Emergency Readiness Team* — **Apple Mac products affected by multiple vulnerabilities.** Apple has released Security Update 2006−004 to correct multiple vulnerabilities affecting Mac OS X, Mac OS X Server, Safari Web browser, Mail, and other products. The most serious of these vulnerabilities may allow a remote attacker to execute arbitrary code. Impacts of other vulnerabilities include bypass of security restrictions and denial−of−service. This security update addresses vulnerabilities in a range of different components, including the handling of a number of different image file formats, ZIP archive files, and HTML Web pages, among others.
Systems affected: Apple Mac OS X version 10.3.9 and earlier (Panther), Apple Mac OS X version 10.4.7 and earlier (Tiger), Apple Mac OS X Server version 10.3.9 and earlier, Apple Mac OS X Server version 10.4.7 and earlier, Apple Safari Web browser, and Apple Mail
Solution: Install Apple Security Update 2006−004:
http://docs.info.apple.com/article.html?artnum=106704
Source: http://www.uscert.gov/cas/techalerts/TA06−214A.html

33. *August 02, Associated Press* — **Experts discuss wireless vulnerability.** Some computers with wireless Internet capabilities are vulnerable to attacks that could expose passwords, bank account details and other sensitive information even if the machines aren't actually online, researchers said at a computer−security conference in Las Vegas, NV, on Wednesday, August 2. The researchers demonstrated the vulnerability, showing how to take complete control of a MacBook from Apple Computer Inc. However, the two researchers, David Maynor and Jon Ellch, said the technique will work on an array of machines, including those that run Microsoft Corp.'s Windows and the free Linux operating system. Maynor and Cache showed a video in which they dropped what is known as a "root kit" into a MacBook by exploiting a weakness found in a wireless card. Maynor was able to create, read and delete files on the Apple laptop. The MacBook, which was running a fully patched version of the latest Apple operating system, showed no indication that it had been compromised. A computer need not be connected to the Internet to be infected. All that's required is that it have certain wireless devices installed and that those devices be turned on.
Source: http://www.nytimes.com/aponline/technology/AP−Wireless−Vulnerability.html?_r=1&oref=slogin

34. *August 02, Associated Press* — **AOL e−mail accounts, software to be free.** In a strategy shift likely to accelerate the decline in its core Internet access business, AOL said Wednesday, August 2, it would give away e−mail accounts and software previously available only to customers who paid as much as $26 a month. AOL hopes to chase additional online advertising dollars instead. Encouraged by such trends as its 40 percent jump in ad revenue in the second quarter, AOL figures that by making services free, it can prevent users from defecting to Yahoo Inc., Google Inc. and Microsoft Corp., which have offered free, ad−supported e−mail for years.
Source: http://www.nytimes.com/aponline/technology/AP−AOLs−Crumbling −Walls.html

35. *August 02, Security Focus* — **Multiple vendor TCP packet fragmentation handling denial−of−service vulnerability.** Multiple vendor implementations of the TCP stack are reported prone to a remote denial−of−service vulnerability. The issue is reported to present itself due to inefficiencies present when handling fragmented TCP packets. The discoverer of this issue has dubbed the attack style the "New Dawn attack"; it is a variation of a previously

reported attack that was named the "Rose Attack". A remote attacker may exploit this vulnerability to deny service to an affected computer.
For a list of vulnerable products, see: http://www.securityfocus.com/bid/11258/info
For solution, see: http://www.securityfocus.com/bid/11258/solution
Source: http://www.securityfocus.com/bid/11258/discuss

36. *August 02, Security Focus* — **Mozilla foundation products XPCOM memory corruption vulnerability.** Various Mozilla foundation products are prone to a memory corruption vulnerability. This issue occurs because the applications, fails to handle simultaneous XPCOM events that would cause the deletion of the timer object. An attacker can exploit this issue to execute arbitrary code.
For a list of vulnerable products, see: http://www.securityfocus.com/bid/11258/info
For solution, see: http://www.securityfocus.com/bid/19197/solution
Source: http://www.securityfocus.com/bid/19197/discuss

37. *August 02, Security Focus* — **Microsoft Windows routing and remote access denial−of−service vulnerability.** Microsoft Windows routing and remote access is prone to a denial−of−service vulnerability. This issue is reportedly due to a NULL pointer dereference error in the affected component. This issue allows remote attackers to cause a denial of service on affected computers.
For a list of vulnerable products: http://www.securityfocus.com/bid/19300/info
Solution: Security Focus is currently not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/19300/discuss

38. *August 02, Security Focus* — **Mozilla Firefox Javascript navigator object remote code execution vulnerability.** Mozilla Firefox is prone to a remote code execution vulnerability. The application fails to properly sanitize user supplied input before using it to create new Javascript objects. Successful exploits may allow an attacker to crash the application or execute arbitrary machine code in the context of the affected application.
For a list of vulnerable products: http://www.securityfocus.com/bid/19192/info
For solution, see: http://www.securityfocus.com/bid/19192/solution
Source: http://www.securityfocus.com/bid/19192/discuss

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 4672 (eMule), 25 (smtp), 54856 (−−−), 19245 (−−−), 6881 (bittorrent), 113 (auth), 445 (microsoft−ds), 6346 (gnutella−svc), 80 (www) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

39. *August 03, Baltimore Sun* — **Door at Baltimore Hebrew University firebombed.** Baltimore police are investigating a firebombing at Baltimore Hebrew University on Wednesday, August 2, after an employee reported a loud noise and then a fire at the base of a side door of a building in Northwest Baltimore. Agent Donny Moses, a city police spokesperson, said the female employee alerted maintenance workers who came and extinguished the small fire and then alerted authorities. Moses said detectives determined the fire was started by an incendiary device, such as a Molotov cocktail, thrown at a steel door, causing no damage. It is being investigated by the department's arson unit, but has not yet been classified as a hate crime. Source: http://www.baltimoresun.com/news/local/crime/bal−fire0803,0,7129549.story?coll=bal−local−headlines

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer